UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/533,061	04/28/2005	Apostolis Salkintzis	CE10337EP	4449

22917 7590 05/16/2008

MOTOROLA, INC.
1303 EAST ALGONQUIN ROAD
IL01/3RD
SCHAUMBURG, IL 60196

EXAMINER	
PACHURA, REBECCA L	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
05/16/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.Schaumburg@motorola.com
APT099@motorola.com

Office Action Summary	Application No.	Applicant(s)	
	10/533,061	SALKINTZIS, APOSTOLIS	
	Examiner	Art Unit	
	Rebecca L. Pachura	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 April 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. The objections to claims 1, 3-25 are withdrawn based on the amendments submitted on 02/27/2008. Claim 2 is objected to because of the following informalities: claim 2 line 1 and line 2 state *"the access port for GPRS communication only"* it should state *"the access* ***point*** *for GPRS communication unit only"*. Appropriate correction is required.

Status of Claims

2. **Claims 1-25 are pending in this Office Action.**

Claims 1-25 are amended.

Response to Amendment

3. **The 35 U.S.C. 112, second paragraph rejection on claim 25 is withdrawn based on the applicant's amendments.**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claim 1-19, 20-22, and 25 rejected under 35 U.S.C. 103(a) as being unpatentable over US 7107620 (Haverinen) in view of US 7239632 (Kalavade).**

As to claim 1, Haverinen discloses (currently amended) a method of authenticating a GPRS communication unit on ~~a~~ GPRS and local network communication systems through an access point of a local network, the method comprising the steps of: the GPRS communication unit attaching to the access point using a local network protocol (Haverinen column 9, lines 56-63). Haverinen fails to teach and combined authenticating the GPRS communication unit with the GPRS network and the local network via a single authentication procedure.

However, Kalavade discloses and combined authenticating the GPRS communication unit with the GPRS network and the local network via a single authentication procedure (Kalavade column 4, lines 8-17 and column 11, lines 35-49).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Haverinen and Kalavade because to authenticate both networks by a single procedure would simplify moving from one network to another (Kalavade column 8, lines 5-60).

The modified Haverinen discloses by communicating GPRS authentication messages between the GPRS communication unit and a GPRS authentication element through the access point by encapsulation of the GPRS authentication messages in local network authentication messages (Haverinen column 31, lines 4-11).

As to claim 2, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating a GPRS communication unit as claimed in claim 1 further comprising the step of ~~authorising~~ authorizing the access port for the GPRS communication unit only if the GPRS communication unit is authenticated by the GPRS authentication element (Haverinen column 22, lines 9-13).

As to claim 3, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the access point requesting an identity from the GPRS communication unit (Haverinen column 2, lines 40-43).

As to claim 4, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 2 wherein the step of authenticating comprises the step of the GPRS communication unit transmitting an identity to the access point (Haverinen abstract).

As to claim 5, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 3 wherein the identity includes a GPRS subscriber identity (Haverinen abstract).

As to claim 6, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the access point communicating an access message to the GPRS authentication element indicating that the GPRS communication unit has attached to the access point (Haverinen column 21, lines 5-13).

As to claim 7, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of ~~the~~ communicating a GPRS Authentication Initiation message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication Initiation message encapsulated in ~~a~~ the local network authentication message from the access point to the GPRS communication unit (Haverinen column 21, lines 13-17 and column 31, lines 4-11).

As to claim 8, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step communicating a GPRS Attach Request message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Attach Request message from the access point to the GPRS authentication element (Haverinen column 8, lines 63-67 and Figure 10 and column 31, lines 4-11).

As to claim 9, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the GPRS authentication element

retrieving authentication data associated with the GPRS communication unit from a Home Location Register (Haverinen column 23, lines 5-12 and Figure 10).

As to claim 10, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the communicating a GPRS Authentication and Ciphering Request message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication and Ciphering Request message encapsulated in ~~a~~ the local network authentication message from the access point to the GPRS communication unit (Haverinen column 23, lines 13-34 and Figure 10 and column 31, lines 4-11).

As to claim 11, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step communicating a GPRS Authentication and Ciphering Response message encapsulated in ~~a~~ the local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Authentication and Ciphering Response message from the access point to the GPRS authentication element (Haverinen column 23, lines 53-63 and Figure 10 and column 31, lines 4-11).

As to claim 12, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the communicating a GPRS Attach Accept message from the GPRS authentication element to the access point, and the step of communicating the GPRS Attach Accept message encapsulated in ~~a~~ the local network authentication message from the access point to the GPRS communication unit (Haverinen column 24, lines 1-24 and Figure 10 and column 31, lines 4-11).

As to claim 13, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of communicating a GPRS Attach

Complete message encapsulated in ~~a~~ the local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Attach Complete message from the access point to the GPRS authentication element (Haverinen column 24, lines 31-33 and Figure 10 and column 31, lines 4-11).

As to claim 14, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of the GPRS authentication element communicating with a Home Location Register to perform a GPRS location update (Haverinen column 19, lines 60-67).

As to claim 15, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the step of communicating an authentication success message from the GPRS authentication element to the access point, and the step of ~~authorising~~ authorizing the access ~~port~~ point for GPRS communication for the GPRS communication unit in response to receiving the authentication success message (Haverinen column 24, lines 5-6).

As to claim 16, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein communication of GPRS authentication messages from the GPRS authentication element to the access point are by encapsulating the GPRS authentication messages in the local network authentication messages (Haverinen column 20, lines 54-62 and column 31, lines 4-11).

As to claim 17, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the authentication is part of a routing area update (Haverinen column 27, lines 40-45).

As to claim 18, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the step of authenticating comprises the steps of: communicating a GPRS

Authentication Initiation message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication Initiation message encapsulated in ~~a~~ the local network authentication message from the access point to the GPRS communication unit (Haverinen column 21, lines 6-8 and column 31, lines 4-11);

followed by the step of: communicating a GPRS Attach Request message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Attach Request message from the access point to the GPRS authentication element (Haverinen column 22, lines 63-67 and column 23, lines 1-4 and column 31, lines 4-11);

followed by the step of: communicating a GPRS Authentication and Ciphering Request message from the GPRS authentication element to the access point, and the step of communicating the GPRS Authentication and Ciphering Request message encapsulated in ~~a~~ the local network authentication message from the access point to the GPRS communication unit (Haverinen column 23, lines 5-34 and column 31, lines 4-11);

followed by the step of: communicating a GPRS Authentication and Ciphering Response message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of communicating the GPRS Authentication and Ciphering Response message from the access point to the GPRS authentication element (Haverinen column 23, lines 53-63 and column 31, lines 4-11);

followed by the step of: communicating a GPRS Attach Accept message from the GPRS authentication element to the access point, and the step of communicating the GPRS Attach Accept message encapsulated in a local network authentication message from the access point to the GPRS communication unit (Haverinen column 24, lines 5-13 and 23-24 and column 31, lines 4-11);

followed by the step of: communicating a GPRS Attach Complete message encapsulated in a local network authentication message from the GPRS communication unit to the access point, and the step of

communicating the GPRS Attach Complete message from the access point to the GPRS authentication element (Haverinen column 24, lines 25-38 and column 31, lines 4-11); and

followed by the step of: communicating an authentication success message from the GPRS authentication element to the access point, and the step of ~~authorising~~ authorizing the access ~~port~~ point for GPRS communication in response to receiving the authentication success message (Haverinen column 24, lines 34-35).

As to claim 19, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the local network is a Wireless Local Area Network (WLAN) (Haverinen column 18, lines 40-44).

As to claim 20, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed claim 15 wherein the Wireless Local Area Network (WLAN) conforms to the Institute of Electrical and Electronic Engineers standard no. 802.1x (Haverinen column 31, lines 4-11).

As to claim 21, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the local network authentication messages are extensible authentication messages (Haverinen Figure 16).

As to claim 22, the modified Haverinen discloses (currently amended) ~~A~~ The method of authenticating as claimed in claim 1 wherein the local network authentication messages are Extensible Authentication Protocol messages (Haverinen Figure 16).

As to claim 25, Haverinen discloses (currently amended) a communication system comprising a GPRS communication network and a local network, the communication system comprising: means for a GPRS communication unit to attach to ~~the~~ an access point using a local network protocol (Haverinen column 9, lines

56-63). Haverinen fails to teach and means for combined authenticating of the GPRS communication unit with the local network and the GPRS network via a single authentication procedure.

However, Kalavade discloses and means for combined authenticating of the GPRS communication unit with the local network and the GPRS network via a single authentication procedure (Kalavade column 4, lines 8-17 and column 11, lines 35-49).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Haverinen and Kalavade because to authenticate both networks by a single procedure would simplify moving from one network to another (Kalavade column 8, lines 5-60).

The modified Haverinen discloses by communicating GPRS authentication messages between the GPRS communication unit and a GPRS authentication element through the access point by encapsulation of the GPRS authentication messages in local network authentication messages (Haverinen column 31, lines 4-11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 7107620 (Haverinen) as applied to claim 1 above, and further in view of US 20030119481 (Haverinen2).**

As to claim 23, the modified Haverinen discloses a method of authenticating as claimed in claim 1. Haverinen fails to teach wherein the GPRS authentication element is a Serving GPRS Support Node (SGSN).

However, Haverinen2 discloses wherein the GPRS authentication element is a Serving GPRS Support Node (SGSN) (Haverinen2 page 2, paragraph 0021).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention an authentication element/server could be a SGSN (Haverinen2 page 2, paragraph 0021).

As to claim 24, the modified Haverinen discloses a method of authenticating as claimed in claim 1. Haverinen fails to teach wherein the GPRS communication unit is a dual-mode communication unit operable to communicate in accordance with a GPRS protocol and a local network protocol.

However, Haverinen2 discloses wherein the GPRS communication unit is a dual-mode communication unit operable to communicate in accordance with a GPRS protocol and a local network protocol (Haverinen2 page 3, paragraph 0037).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention that if the terminal/GPRS communication unit could operate in dual-mode then it would not matter what the protocol was (Haverinen2 page 3, paragraph 0037).

Response to Arguments

6. Applicant's arguments filed 02/27/2008 have been fully considered but they are not persuasive.

Applicant has presented amendments for the 35 U.S.C. 112, second paragraph rejection, and has made some amendments for clarification. Applicant has made arguments for the rest of the response, see below.

The Applicant Argues:

Independent claim 1 has been amended to reflect that the present invention addresses a different issue than Haverinen, and it is novel in that it discloses a unique method that can be used by a GPRS communication unit in an integrated GPRS/WLAN network in order to perform combined WLAN authentication and GPRS authentication to achieve simultaneous authentication on two systems. Support for this can be found in the

specification on page 5 lines 16-18, and page 13 lines 20-22. A novel aspect of applicant's invention is the fact that the two authentication procedures (for WLAN and GPRS) are consolidated into a single authentication procedure. Haverinen is only concerned with authentication in one communication system and therefore could not envision either the problem of authentication on two systems or applicant's novel solution for combined authentication on two systems using a single procedure.

The major benefit of applicant's disclosed combined authentication method is that handover from GPRS to WLAN is performed considerably faster because the WLAN authentication procedure and the GPRS authentication procedure are not sequentially executed, but rather they are combined into a single authentication procedure (shown in Fig. 4 of the present invention). This can bring considerable benefits to real-time applications, which cannot tolerate large latency during handover.

Haverinen does not consider how to combine the WLAN authentication procedure with the GPRS authentication procedure but instead considers how to authenticate a communication device on a single data network. Haverinen does not disclose or suggest a reason to combine the WLAN and the GPRS access control procedures as does the present invention. At best, Haverinen could only consider authentication procedures as separate, and therefore could only envision executed one authentication procedure on one data network followed by another authentication procedure on another network, and thereby suffers from high handover latencies.

In addition, Haverinen does not assume that a WLAN can enforce IEEE 802. lx access control and therefore its applicability is limited only to single packet data networks. As noted above, the advantage of the present invention with respect to Haverinen is that it provides the means for fast handover from GPRS to WLAN. In addition, the protocol architecture proposed by Haverinen (as per Figs. 2 or 10 of Haverinen) and the protocol architecture proposed by the present invention (as per Fig. 3 of the present invention) are completely different.

This fact reinforces applicant's argument that the present invention addresses and solves a different issue than the one addressed in C.

In response, the examiner respectfully submits:

Based on the addition of the reference Kalavade in response to the applicant's amendments; this argument is moot.

The Applicant Argues:

Moreover, Haverinen does not disclose or suggest the encapsulation of an authentication message of one network protocol into an authentication message of another network protocol.

Therefore, applicant respectfully submits that amended claim 1 is patentable and non- obvious over Haverinen. Claim 25 has been amended similarly to claim 1 and is therefore deemed inventive as well, for the same reasons.

Regarding claim 7, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 21 lines 13-17) discloses the encapsulation of an authentication message of one network protocol into an authentication message of another network protocol. Instead this reference only recites how a single authentication procedure is triggered by software.

Similarly for claim 8, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 8 lines 63-67 and Fig. 10 step 401) discloses the encapsulation of an authentication message of one network protocol into an authentication message of another network protocol. Instead this reference only recites a request to start a single authentication procedure.

Similarly for claim 10, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 23 lines 13-34 and Fig. 10 step 404) discloses the encapsulation of an authentication message of one

network protocol into an authentication message of another network protocol. Instead this reference only recites the encryption of authentication in a single network protocol a response to a request to start a single authentication procedure.

Similarly for claim 11, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 23 lines 53-63 and Fig. 10 step 421) discloses the encapsulation of an authentication message of one network protocol into an authentication message of another network protocol. Instead this reference only recites the sending of an answer to a request to start a single authentication procedure.

Similarly for claim 12, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 24 lines 1-24 and Fig. 10 steps 424, 431,441,442, 451,452) discloses the encapsulation of an authentication message of one network protocol into an authentication message of another network protocol. Instead this reference only recites providing an access key in a response for a single authentication procedure.

Similarly for claim 13, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 24 lines 31-33 and Fig. 10) discloses the encapsulation of an authentication message of one network protocol into an authentication message of another network protocol. Instead this reference only recites a term for re-authentication for a single authentication procedure.

Similarly for claim 16, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 20 lines 54-62) discloses the encapsulation of an authentication message of one network protocol into an authentication message of another network protocol. Instead this reference only discloses one network protocol for authentication for a single authentication procedure.

Similarly for claim 18, applicant respectfully disagrees with the Examiners contention that Haverinen (col. 21 lines 6-8, col. 22 lines 63-67, col. 23 lines 1-34 and 53-56, col. 24 lines 5-13 and 23-38 and Fig. 10 steps 401,402, 403,404, 411,412, 421,422, 431,452, 453) discloses the encapsulation of an authentication

message of one network protocol into an authentication message of another network protocol. Instead this reference only recites a single network protocol for a single authentication procedure.

In response, the examiner respectfully submits:

Haverinen does teach encapsulation over LAN protocol (Haverinen column 31, lines 4-11).

The Applicant Argues:

Claims 20, 23 and 24 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Haverinen in view of US 2003/0119481 (Haverinen2). This rejection is respectfully traversed.

Applicants respectfully submit that independent claim 1 has been amended into a condition for allowance as detailed above.

Claims 20, 23 and 24 are dependent on amended claim 1, hereby incorporated be reference, and are therefore deemed allowable as well for the same reasons.

Accordingly, it is respectfully submitted that this rejection has been overcome.

In response, the examiner respectfully submits:

Based on the addition of the reference Kalavade in response to the applicant's amendments; this argument is moot.

Based on the examiner's arguments claims 1-25 are rejected under 35 U.S.C. 103(a).

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this

final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm est.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/
Examiner, Art Unit 2136

/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135